03/07/05

AF ZMW

Practitioner's Docket No. None

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Ralph V. Bain		
Application No.:	09/707225	Group No.:	2136
Filed:	11-04-2000	Examiner:	Pramila Parthasarathy
For:	Self-Decrypting Web Site Pages		

Mail Stop Appeal Briefs-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANT'S BRIEF (37 C.F.R. § 1.192)

This brief, which is transmitted in triplicate, is in furtherance of the Notice of Appeal, filed in this case on 1-10-2005.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10

I hereby certify that, on the date shown below, this correspondence is being deposited with the United States Postal Service as Express Mail in an envelope addressed to Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Mailing Label No. ED 040376829 US

Ralph V Bain

Signature

Ralph V. Bain

Date: March 5, 2005

03/08/2005 MAHMED1 00000015 09707225

01 FC:2402 250.00 OP

I REAL PARTY IN INTEREST

The real party in interest in this appeal is the party named in the caption of this brief, namely Ralph V. Bain.

II RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences which will directly affect, or be directly affected by, or nave a bearing on the Board's decision in this appeal.

III STATUS OF CLAIMS

The status of the claims in this application is:

TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-9

STATUS OF EACH CLAIM

Claim 1 (rejected)
Claim 2 (rejected)
Claim 3 (rejected)
Claim 4 (canceled)
Claim 5 (rejected)
Claim 6 (rejected)
Claim 7 (rejected)
Claim 8 (rejected)
Claim 9 (rejected)

C. CLAIMS ON APPEAL

The claims on appeal are: 1-3 and 5-9

IV STATUS OF AMENDMENTS

The Amendment After Final filed on 12 November 2004 was ultimately entered, but only after intervention by the Examiner's acting Supervisor, as will be explained in detail below.

For purposes of this appeal, Appellant has included the amendments to claims 1, 2, and 5 contained in the Amendment After Final.

V SUMMARY OF INVENTION

Overview

The Appellant's invention is a method for automatically operating a decryption function within a web site page, as defined in Claim 1. This decryption function decrypts a cryptogram that is contained within a web site page as that page is being displayed to a web site visitor. The major elements of the invention are the web site page, the cryptogram, certain data within the web site page for validating associated keys for the cryptogram, and the decryption function itself, which automatically activates as the web site page is being displayed. Appellant's method operates completely within the confines of the web site page, receives and validates the key for the cryptogram, and produces a decrypted version of the cryptogram. The decrypted version of the cryptogram is then available for display using the industry-standard method. With this method, each web site page in a web site will have self-decrypting capabilities.

Features defined in Appellant's dependent claims provide additional and significant benefits to those who utilize Appellant's **method for automatically operating a decryption function within a web site page** in their web site operations, as listed below:

Claim 2. The cryptogram within the web site page is decrypted and displayed "in place," so the original continuity and placement of the normal clear text in a page relative to the encrypted text (cryptogram) in that page will be preserved in the final display of the page.
Claim 3. The cryptogram can be as small as a single character, or as large as the entire displayable portion of a standard web site page.
Claim 5. Within the same page, a set of different keys can be used to decrypt a set of corresponding different cryptograms.
Claim 6. The web site visitor directly provides the above keys to the decryption function. As a result, the visitor determines which of the cryptograms within a page are decrypted and displayed.
Claim 7. The web site visitor receives an immediate validity report directly from the decryption function as each key is entered, and does not have to wait for a communication from a server system.
Claim 8. The web site visitor only needs to enter keys once, and they will all be made available for decrypting cryptograms in each and every page that is browsed within the chosen web site.
Claim 9. If a web site visitor browses a site without downloading a page containing at least one cryptogram, this visitor is provided the convenience of not being asked to enter keys.

In addition to the above benefits, a **self-decrypting web site page** provides a profound security improvement associated with publishing sensitive information in web site pages that are distributed on the open Internet. These benefits derive from the fact that, in current practice, "secure" web site pages are only encrypted while they are being transmitted between the web site host server and the site visitor's browser. At all other times, the pages and received copies thereof are stored and exposed on the server and visitors' systems in clear text. This is **not** the case with Appellant's self-decrypting web site pages, since the cryptograms within these pages are created along with the original creation of the page, and **remain as cryptograms** at all times while the pages are stored on the server or site visitor's systems, even while site visitors view decrypted versions of the cryptograms on a monitor.

Appellant's recent search of prior art and the latest product announcements for established web site browsers discloses nothing that equates to the operational characteristics, capabilities, or benefits of Appellant's **method for automatically operating a decryption function within a web site page**.

Drawings and Descriptions in Support of Appellant's Claims

NOTE: All references to Appellant's program code listing shown in Figs. 7-A through 7-F use the same reference numbers that are used in Appellant's Figures 1 through 6 and specification.

The basis for **Claim 1** can be found in an overview of the elements of the invention found in:
Fig. 1-A (Ref#s. 101 >> 111)
Specification (page 5 - line 22 >> page 6 - line 3) and
Fig. 6 (Ref#s. 100 >> 111 and 200)
Specification (page 11 - line 10 >> page 12 - line 6).

The basis for **Claim 2** can be found in:
Fig. 1-A (Ref#s. 110, 111, 114)
Specification (page 5 line 29 >> page 6 line 3),
Fig. 1-B (Ref#s. 121, 122, 123)
Specification (page 6 lines 4 >> 17)
Program listing (Fig. 7-F sections: 121, 122, 123), and
Fig. 5 (Ref#. 510, 512)
Specification (page 10 line 31 >> page 11 line 2)
Program listing (Fig. 7- E section: 510, 512).

The basis for **Claim 3** can be found in:
Fig. 1-A (Ref#s. 110, 111, 114)
Specification (page 5 line 27),
Fig. 1-B (Ref#s. 121, 122, 123)
Specification (page 6 lines 4 >> 9)
Program listing (Fig. 7-F sections: 121, 122 123), and
Fig. 5 (Ref#s. 510, 512)
Specification (page 10 line 31 >> page 11 line 11)
Program listing (Fig. 7-E section: 510, 512).

Claim 4 is canceled.

The basis for **Claim 5** can be found in:
Fig. 3-B (Ref#s. 312, 314, 316)
Specification (page 8 line 31 >> page 9 line 7)
Program listing (Fig. 7-B section: 312, 314, 316), and
Fig 4-A (Ref#. 402) and Fig. 4-B (Ref#s. – All)
Specification (page 9 line 9 >> page 10 line 6)
Program listing (Fig. 7-B sections: 402, 404, 406, 408, 410) and (Fig. 7-C sections: All).

The basis for **Claim 6** can be found in:

Fig. 6 ("Web Site Viewers Keyboard Input"),

Fig. 3-B (Ref#s. All)

Specification (page 8 line 16 >> page 9 line 5)

Program listing (Fig. 7-A sections 305, 306, 316) and (Fig. 7-B sections: 308 >> 316), and

Fig. 4-A (Ref#. 402) and Fig. 4-B (Ref#s. – All)

Specification (page 9 line 9 >> page 10 line 6)

Program listing (Fig. 7-B sections: 402 >> 410) and (Fig. 7-C sections: All).

The basis for **Claim 7** can be found in:

Fig. 4-B (Ref#s. 416, 418)

Specification (page 9 line 25 >> page 10 line 6)

Program listing (Fig. 7-C sections: 416, 418).

The basis for **Claim 8** can be found in:

Fig. 6 (Ref#. 200),

Fig. 2 (Ref#s. All)

Specification (page 6 lines 20 >> 30)

Program listing (Fig. 7-G sections: All),

Fig. 4-B (Ref#. 418)

Specification (page 10 lines 1 >> 6)

Program listing (Fig. 7-B section: 308) and (Fig. 7-C section: 418),

Fig. 5 (Ref#. 504)

Specification (page 10 lines 14 >> 25), and

Program listing (Fig. 7-D section: 504, 512).

The basis for **Claim 9** can be found in:

Fig. 6 (Ref#. 101, 102, 111)

Specification (page 11 line 23 >> page 12 line 3), and

Fig. 3-B (Ref#. 305, 306, 316)

Specification (page 8 lines 16 >> 30)

Program listing (Figs. 7-A sections: 305, 306, and 316).

VI ISSUES

A. Whether the Examiner errs technically by assuming that a browser is the same as a web site page, that Appellant's cryptogram is the same as the HTML Form in Chang (U.S. Patent No. 6,105,012, hereinafter "Chang"), and that Appellant's associated key is the same as Chang's session key.

B. Whether claims 1-3 and 5-9 are unpatentable under 35 U.S.C. § 102(e) as being anticipated by Chang.

VII GROUPING OF CLAIMS

Since the ground of rejection for all Appellant's claims involves only 35 U.S.C § 102(e), Appellant holds that all claims fall into the same group.

VIII ARGUMENTS–REJECTIONS UNDER 35 U.S.C. § 102(e)

Introduction

This introduction is presented to show some of the problems which Appellant has encountered during the examination process.

A. In the first Office Action (04-09-2004), over 3½ years after the application was filed, all of Appellant's claims were rejected under 35 U.S.C. § 103(a) as being unpatentable over Chang in view of Lincke et al (U S Patent No. 6,253,326 hereinafter "Lincke"). In this Office Action, the Examiner simply repeated Appellant's claims, inserting references to Chang and Lincke, but did not provide any rationale for finding correspondence between Appellant's claims and the referenced material which, in every case, is clearly **not related** to Appellant's claimed subject matter..

B. In response, Appellant amended claim 1 to its present form and removed all references to a browser. Appellant also pointed out the new and unexpected results of each claim.

C. In the second Office Action (10-13-2004) which was made Final, all of Appellant's claims were rejected under 35 U.S.C § 102(e) as being anticipated by Chang. Once again, there was no rationale provided for the Examiner's findings. The Examiner also objected to claims 1 and 5 because of informalities and concluded that "appropriate correction is required."

D. In an Amendment After Final which was filed within two months of the mailing of the Final Action, Appellant pointed out that anticipation was not possible because each and every element of Claims 1-3 and 5-9 are not disclosed by Chang. Claims 1 and 5 were amended to correct the typographical error which the Examiner was kind enough to point out, and Claim 2 was amended for further clarification.

E. In the first Advisory Action (12-03-2004) Appellant's claims were again rejected, with references being made both to Chang and Lincke, which reference to Lincke was improper because of the anticipation rejection which can only be based upon a single reference. The Examiner once again provided no rationale to support the findings. The Examiner repeatedly stated that Appellant's "arguments are not found persuasive" and referred to the same and different portions of Chang. Also, the cover sheet for this Advisory Action did not show whether or not the proposed amendments made by Appellant in the Amendment After Final would be entered for the purposes of appeal.

F. Appellant telephoned the Examiner (on or about 12-08-2004) to ask why the Advisory Action did not specify whether the amendments would or would not be included for purposes of appeal.

G. The Examiner faxed a second Advisory Action cover sheet to Appellant (12-09-2004) which indicated that the amendments would **not** be included. This meant that the Examiner would not even enter the amendments to claims 1 and 5 which corrected typographical errors which the Examiner had previously stated required appropriate correction!

H. Appellant then called Acting Supervisor Albert Dekadi (on or about 12-12-2004) to ask why the amendments would not be included, and also to explain that Appellant was having difficulty formulating arguments because there was no rationale for the Examiner's findings.

I. Appellant then received a revised third Advisory Action (12-21-2004) which indicated that Appellant's amendments **will** be included for the purposes of appeal. Also, the Examiner's arguments include more detail and rationale on how comparisons were made between Appellant's claims and Chang's specification.

Appellant submits that throughout the examination and amendment process, the Examiner failed to adequately identify the disclosures in Chang which were deemed to show anticipation of Appellant's invention, and has otherwise failed to provide a rationale for rejection of Appellant's claims. As a result, the Examiner heretofore has prevented Appellant from formulating precise and effective arguments against the Examiner's assertions with regard to Chang's anticipation. Only now can this be attempted after receipt of the third Advisory Action.

Issue A

With the recent expanding of the Examiner's arguments, they now clearly show that the Examiner's rejections of Appellant's claims are based on incorrect technical pre-conceptions and inaccurate interpretations, as listed below:

A. With regard to computer system architecture, the Examiner incorrectly assumes that a computer **web site page** is the same as a computer **browser** (Third Advisory Action Page 5 lines 8-10) even though there is no support for this assumption in either Appellant's claims or Chang's specification. Also, it is well known that a web site page is an HTML **data file**, a browser is a **computer program** that **processes** data files, and the two of them are completely different entities with different characteristics and purposes within the computer system realm. The seriousness of the incorrect assumption on the part of the Examiner is made apparent in Appellant's arguments for Claim 1, where it is clear that the Examiner argues for anticipation of **a method for automatically operating a decryption function within a web site page** by referring to disclosures of Chang's **browser** capabilities.

B. With regard to Appellant's and Chang's system elements, the Examiner (Third Advisory Action Page 2 lines 12-16) incorrectly assumes the following:

   1. That Appellant's cryptogram (Defined in Claim 1) is the same as Chang's **HTML Form** (Chang Column 11 lines 15-34). This is discussed further in Appellant's arguments for Claim 1.
   2. That Appellant's **associated key** (Defined in Claim 1) is the same as Chang's **session key** (Chang Column 5 lines 23-29 and Column 9 lines 48-51). This is discussed further in Appellant's arguments for Claim 1.

C. In addition, some the Examiner's arguments are based on material that does not exist in the Examiner's references to Chang or, for that matter, anywhere else in Chang's specification. These occurrences are detailed in Appellant's arguments.

Appellant submits that the Examiner's omissions, misconceptions, and inaccuracies have skewed the examination process, because there is nothing in Chang's specification that is a proper basis for rejection of any of Appellant's claims.

Issue B

Chang's level of detail is not sufficient to provide a basis for anticipation of Appellant's invention

A careful comparison of Appellant's and Chang's inventions shows that Chang has a different and broader purpose and a much greater scope than Appellant. Chang therefore, in his figures and specification, discloses the "steps" in his method in terms of the final results of lower-level functions, without disclosing the detailed steps involved in those functions. Appellant submits that Chang's specification does not disclose any method at the level of detail needed to anticipate Appellant's **method for automatically operating a decryption function within a web site page.** A specific example:

A. Chang's **Figure 15A** step **382**, and **Figure 15B** steps **414** and **416** disclose the decryption function that is contained in his browser program for decrypting web site pages. Chang's specification uses only 10 lines **(Column 11 lines 39-48)** and only a few key words to describe the above three steps and disclose his entire browser decryption function. Chang does **not** disclose the inner workings of the function, nor the multitude of steps involved. Essentially, Chang discloses only that a decryption function exists in a browser, as is already well known.
B. In contrast, Appellant's **entire** set of figures and specification are completely devoted to the intricacies of operating a decryption function within a web site page, and they disclose (even to the program code level) all of the steps necessary to make Appellant's novel function operate properly.

Chang does not disclose a method for a decryption function within a web site page, nor does Chang even disclose the method for operating the decryption functions **in his own server and browser programs.** There is no basis in Chang for anticipation of any portion of Appellant's invention.

Disclosure of each and every element

As is well known, under 35 U.S.C. § 102(e), anticipation requires that each and every element of the claimed invention be disclosed in one prior art reference. In the Third Advisory Action, the Examiner asserts that such disclosures exist in Chang's specifications for each and every one of Appellant's claims, using arguments which contain references to Chang's specification. Appellant submits that the Examiner errs in finding such disclosures in Chang's specification, and that Appellant's Claims 1-3 and 5-9 are patentable.

The Rejection of Claim 1

Appellant submits that the Examiner errs in rejecting Appellant's claim 1, as explained below:

The Examiner states that even the preamble of **Claim 1** is anticipated by Chang (Third Advisory Action Page 2 lines 11-13) citing references as follows:

A. (Chang Column 2 lines 20 – 45) which discloses only that Chang's **browser** element has decryption capability, and does **not** disclose any capability for **operating a decryption function within a web site page**, as defined in the preamble to Claim 1. Chang clearly does not anticipate this most fundamental aspect of Appellant's claimed method, which is also the foundation for all of the operational features and benefits provided by Appellant's invention.

B. (Chang Column 9 lines 5 – 51) which discloses only that Chang's **server** element decrypts data within messages that are sent up from the browser element. Once again, there is no disclosure of any type of **decryption function** or any other process that operates **within a web site page**, and therefore there is no anticipation of the preamble of Claim 1 by Chang.

C. (Chang Column 12 lines 37 – 49) is an overall summary of Chang's invention. This summary does not disclose the methods or processes used within any of the elements of Chang's system, and therefore it does not anticipate any aspect of the preamble of Claim 1.

D. In addition, Chang's specification elsewhere discloses **only** that his **decryption** takes place within system elements **other** than his **web site page**, namely in the server and browser as shown below:

1. In Chang's Figure 15A where the logic diagram discloses the **web browser** receiving an HTML document **380**, he clearly discloses in the first decision box **382** that when an HTML document needs decryption, the **web browser** branches internally to **414** and **416** in Fig. 15B and **decrypts** the data in the document.
2. In Chang (Column 4 lines 55-60) under **web server procedures 120** Chang discloses an encryption procedure **126** for encrypting and **"decrypting data."**
3. In Chang (Column 5 lines 23-27) he discloses "The **web browser 216** can contain the following: one or more user encryption keys **218** for randomly generating session keys; an encryption procedure for encrypting and **decrypting data**; . . ."
4. In Chang (Columns 10 lines 45-47) he discloses: "Thus, **the web browser decrypts** the key from the known location . . ."
5. In Chang (Columns 11 lines 1-2) he discloses: "**The server decrypts** and verifies the information in the received registration message."
6. Chang's (Column 11 lines 34-48) states "The web browser **216** reads the data from the file until it reaches the corresponding FORM tag pair (i.e. </FORM>) (step **414**). **The web browser 216 decrypts** the form with the user's private key . . ."

E. Furthermore, Chang **claims** that his decryption functions reside in his web browser and his server (Claims 16, 21, and 25), and does **not** claim that such a function resides **within a web site page**.

Merely referring to the browser and server of Chang can not anticipate the preamble of Claim 1, which calls for a **method** for automatically operating a decryption function within a web site page.

The Examiner argues against **element (b) of Claim 1** in Page 2 lines 13-15 of the Third Advisory Action.

> The Examiner includes the phrase "... encrypted HTML form (cryptogram), ..." thus equating Chang's "encrypted HTML form" with Appellant's "cryptogram." This is a misconception. (Chang Column 11 lines 39-43) discloses that it is the **data within** the HTML form that is decrypted, indicating that his cryptogram is **not** his encrypted HTML form, as stated by the Examiner, but is instead his encrypted HTML Form **data** -- a significantly different entity. Thus, the Examiner does not seem to know what Chang's browser is really decrypting. But even when Chang's cryptogram is properly identified, his specification still does not disclose the construction of Appellant's cryptogram in such a form (Appellant's Fig. 1-B) that it can be decrypted by a **decryption function within the web site page**.

Since Chang does not anticipate element (b) of Claim 1, this claim cannot be properly rejected under § 102(e).

The Examiner argues against **element (c) of Claim 1** in Page 2 lines 13-15 of the Third Advisory Action.

A. There is no disclosure whatsoever in Chang's entire specification that discloses or even suggests that data is placed **within a web site page** to validate a key.
B. The Examiner includes the phrase "... session key (associated key) ..." thus equating Chang's "session key" with Appellant's "associated key." This is an error in two ways. First, Chang (Column 11 lines 44-47) discloses that his system utilizes the **user's private key** for decrypting his forms, **not** the session key. Second, **none** of the many types of Chang's keys are equivalent to Appellant's **associated keys**, which are entered directly into a web site page (Claim 6), validated **within a web site page** – (Claims 7 and 1(c)), and used to decrypt associated cryptograms **within each of a plurality of web site pages** (Claim 5).

Since Chang does not have element (c) of Claim 1, Chang cannot anticipate Claim 1.

The Examiner does not even argue against **element (d) of Claim 1.**

> This element is the major defining element in all of Appellant's claims. The failure of the examiner to refer to Chang and argue against this element is consistent with Appellant's finding that Chang's specification makes no disclosure whatsoever regarding **a method for automatically operating a decryption function within a web site page** as defined in Claim 1.

Since the Examiner has failed to argue against element (d) of Claim 1, it cannot be used as a basis for a § 102(e) rejection.

Claim 1 is Not Anticipated by Chang

Appellant has clearly shown that Chang teaches and describes that his web browser and server are the **sole** system elements in which his decryption functions reside. Chang's figures and specifications do **not** teach or describe that a decryption function or any of its elements operate or reside within a web site page. No wonder the Examiner has not successfully argued that each and every element of Claim 1 is anticipated by Chang, Therefore, Appellant submits that there is no basis for rejection of Claim 1 under § 102(e) and requests reconsideration and allowance. Appellant has persuasively argued that Claim 1 is patentably distinguishable from Chang.

The Rejection of Dependent Claims 2-3 and 5-9

The Examiner argues against Claim 2 (Third Advisory Action Page 3 lines 10-19) citing Chang as follows:
(Column 8 lines 7-20)

A.) The Examiner gravely misquotes this reference by using the word "session" in place of the word "account" that is used in the reference, and by using the words "decrypted version" (from Appellant's Claim 2) that do not appear in this reference. The Examiner's statement of what this reference discloses is not factual, and the argument has no merit.

B. Also, a careful examination of this reference finds **no** disclosure of **multiple** decrypted cryptograms (Chang's form data) within **each** web site page (Chang's HTML form), as defined in the first portion of Appellant's Claim 2.

(Column 9 lines 49-53)

The Examiner fails to note that this reference discloses the operation of Chang's **Financial Server**, which **decrypts** only **messages**, and does **not decrypt web site pages**. The entire reference is unrelated to Appellant's claim 2 subject matter.

The Examiner fails to cite any references in Chang that would show anticipation of the second portion of Appellant's Claim 2.

A careful examination shows nothing in Chang's specification disclosing that the decrypted versions of HTML Form data (Chang's cryptograms) are displayed in the original position that the encrypted HTML Form data occupied within a web site, as claimed in the second portion of Appellant's Claim 2.

Additionally, nowhere in Chang's specification does he teach that the functionality defined in Appellant's Claim 2 results from **automatically operating a decryption function within a web site page,** as defined in Appellant's Claim 1.

Appellant submits that Claim 2 is not anticipated by Chang.

The Examiner argues against Claim 3 (Third Advisory Action Page 4 lines 4-8) citing Chang as follows:
(Column 2 lines 30-38 and Column 4 lines 2-20)

A. These references do **not** address in any way the **size** limits of HTML documents, HTML Forms, or HTML Form data (Chang's cryptogram). Chang only discloses the handling of HTML documents and HTML forms, and discloses nothing related to the size of his cryptogram in comparison to the size of the **body** of the HTML document containing his cryptogram, as defined in Appellant's Claim 3.

B. In addition, these references do not disclose a **minimum** size for cryptograms. Appellant's cryptograms can be a single character (**"... <u>any</u> size up to ..."**). These references do not anticipate Appellant's Claim 3.

Additionally, nowhere in Chang's specification does he teach that the functionality defined in Appellant's Claim 3 results from **automatically operating a decryption function within a web site page,** as defined in Appellant's Claim 1.

Appellant submits that Claim 3 is not anticipated by Chang.

Claim 4 - Canceled

The Examiner argues against Claim 5 (Third Advisory Action Page 4 lines 14-18) citing Chang as follows:
(Column 5 lines 20-45)

In the Examiner's argument against Claim 5, the Examiner gravely misquotes and incorrectly interprets this reference to Chang, as described below:

1. This reference clearly discloses that the session key is used to **encrypt** return messages to the server, and **not** "**decrypt** HTML documents" as stated by the Examiner.
2. This reference in Chang does not mention "HTML documents" at all.
3. The Examiner incorrectly equates Chang's **forms** and Appellant's **cryptograms** – See Claim 1, Appellant's argument against Third Advisory Action (Page 2 lines 13-15).
4. The Examiner incorrectly equates Chang's **session key** and Appellant's **associated key** – See Claim 1, Appellant's argument against Third Advisory Action (page 2 lines 13-15).
5. There is nothing in this reference disclosing that the keys used for decrypting the web page's cryptograms are obtained **from a plurality of such keys**, as in Appellant's Claim 5.
6. There is nothing in this reference disclosing that each web site page, **within itself**, contains the means for **independently decrypting a plurality of cryptograms**, as in Appellant's Claim 5.

Additionally, nowhere in Chang's specification does he teach that the functionality defined in Appellant's Claim 5 results from **automatically operating a decryption function within a web site page,** as defined in Appellant's Claim 1**.**

Appellant submits that Claim 5 is not anticipated by Chang.

The Examiner argues against Claim 6 (Third Advisory Action Page 5 lines 14-18) citing Chang as follows:
(Column 5 lines 23-45 and Column 6 lines 57-64)

A. The Examiner again incorrectly equates Chang's **session key** and Appellant's **associated key** – See Claim 1, Appellant's argument against (Third Advisory Action Page 2 lines 13-15).
B. Chang does not disclose a human operator as part of his system, and even though this is acknowledged in the Examiner's argument, the Examiner continues to argue separately that a **human server operator** could manage keys for web sites. As a result, the Examiner's imagination, rather than Chang's specification, is used as a basis for rejection. In addition, it is well known that the client users (those who are browsing web sites) are the only humans immediately involved in managing their web site visits, and that a **human server operator**, if such existed, would never be able to enter keys for the thousands of visitors who might be accessing the same server at any given time. The Examiner's notion is not reasonable, and since it is also **not** expressly disclosed in Chang, it cannot be a basis for rejection under § 102(e).
C. A method for entering keys directly into a web site page is **not** disclosed anywhere in Chang's specification. Therefore, there is no anticipation of a human operator providing such keys as defined in Appellant's claim 6.

Additionally, nowhere in Chang's specification does he teach that the functionality defined in Appellant's Claim 6 results from **automatically operating a decryption function within a web site page, wherein said decryption function obtains said associated key from a plurality of said associated keys** as defined in Appellant's Claim 5.

Appellant submits that Claim 6 is not anticipated by Chang.

The Examiner argues against Claim 7 (Third Advisory Action Page 6 lines 1-5)...
... citing the Examiner's "Claim 6 reasons for a human operator."

Appellant's arguments for Claim 6 show that the Examiner's reasons for a human operator are contrived and have no merit.

... citing Chang(Column 11 line 60 to Column 12 line 10).

This reference discloses a method whereby the browser in Chang's system prepares return messages (Chang column 11 lines 55-60) for transmission to the server. There is no relationship between this process (or its purpose) and the Appellant's process for providing a key validity report to a human operator. And even though the Examiner states in the above cited argument that "Chang teaches human operator receives a validity report ...," a careful examination of this reference clearly shows that the words "validity", "report", "human", and "operator", are never used in this reference. The Examiner's argument has no merit.

Additionally, nowhere in Chang's specification does he teach that the functionality defined in Appellant's Claim 7 results from **automatically operating a decryption function within a web site page, wherein said decryption function obtains said associated key from a plurality of said associated keys, wherein a human operator provides said plurality of said associated keys**, as defined in Appellant's Claim 6.

Appellant submits that Claim 7 is not anticipated by Chang.

The Examiner argues against Claim 8 (Third Advisory Action Page 6 lines 14-20)...
... citing the Examiner's "Claim 6 reasons for a human operator."

Appellant's arguments for Claim 6 show that the Examiner's reasons for a human operator are contrived and have no merit.

... citing Chang(Column 1 line 66 to Column 2 line 55).

A. This reference provides an overview of browser/server interactions and related message handling. Contrary to the Examiner's argument, this reference is not related in any way to the distribution of keys to web site pages.

B. A key element of this claim is the well-known and well-defined HTML Frameset Page, which is a special type of web site page that is optionally downloaded as the first page in a web site. The Frameset Page, among other things, enables data communications between all the other pages in the web site, which is an absolute requirement in Appellant's invention. Contrary to the Examiner's statement, Chang does **not** teach the use of a Frameset Page, nor are the words "Frameset Page" found anywhere in his specification.

Additionally, nowhere in Chang's specification does he teach that the functionality defined in Appellant's Claim 8 results from **automatically operating a decryption function within a web site page, wherein said decryption function obtains said associated key from a plurality of said associated keys, wherein a human operator provides said plurality of said associated keys**, as defined in Appellant's Claim 6.

Appellant submits that Claim 8 is not anticipated by Chang.

The Examiner argues against Claim 9 (Third Advisory Action Page 7 lines 6-12)...
... citing the Examiner's "Claim 6 reasons for a human operator"

Appellant's arguments for Claim 6 show that the Examiner's reasons for a human operator are contrived and have no merit.

... citing Chang(Column 2 lines 56-66).

A careful examination of this reference shows that it is related only to Chang's Financial **Server** process for handling messages that are **uploaded** from his browser to his server. This process is completely unrelated to Appellant's logical mechanism for detecting and taking action on the first cryptogram that is **downloaded** by a web site server as the site is visited. Also, contrary to the Examiner's statement, this reference never mentions a human operator, a cryptogram, or a web site. This reference shows no anticipation of Claim 9 in Chang.

... citing Chang(Column 8 line 60 to Column 9 line 3).

A careful examination of this reference shows that it is related only to another process in Chang's Financial **server** which registers a user for a server/client transaction session. This process is not related in any way to Claim 9. Also, contrary to the Examiner's statement, this reference never mentions a human operator, a cryptogram, or a web site. This reference shows no anticipation of Claim 9 by Chang.

Additionally, nowhere in Chang's specification does he teach that the functionality defined in Appellant's Claim 9 results from **automatically operating a decryption function within a web site page, wherein said decryption function obtains said associated key from a plurality of said associated keys, wherein a human operator provides said plurality of said associated keys**, as defined in Appellant's Claim 6.

Appellant submits that Claim 9 is not anticipated by Chang.

Appellant submits that none of the elements of Claims 2-3 and 5-9 are disclosed or even suggested by Chang, therefore anticipation is not possible, and Appellant's Claims 2-3 and 5-9 are patentably distinguishable from Chang.

35 U.S.C. 102(e) states that a person is entitled to a patent unless --- the invention was described in (1) an application for patent ... or (2) a patent granted on an application for patent ... . In light of the foregoing failings of the Chang patent with regard to the method of the present application and in the claims under appeal, it is respectfully submitted that the claimed invention has not been described in Chang prior to the present application as contemplated by the above statutory provision. The Appellant should therefore be entitled to a patent.

The Appellant has spent a great deal of time in developing the method for automatically operating a decryption function within a web site page claimed in the Claims here under appeal. His invention is not found in the references cited by the Examiner. The rejection of these claims based on Chang is believed to be improper.

It is submitted that the Final Rejection should not be sustained and that Claims 1-3 and 5-9 of this application should be allowed.

Date: March 5, 2005

Ralph V. Bain
SIGNATURE OF APPELLANT

Ralph V. Bain

Tel. No.: (510) 657-6384

39908 San Simeon Ct.
P.O. Address

Fremont, CA 94539-3619

IX APPENDIX OF CLAIMS

Claim 1: A method for automatically operating a decryption function within a web site page, comprising:

(a) providing said web site page,

(b) providing a cryptogram within said web site page,

(c) providing the data within said web site page for validating an associated key for said cryptogram, and

(d) providing said decryption function within said web site page which will:

(1) automatically activate as said web site page is being displayed,

(2) execute within the confines of said web site page,

(3) receive and validate said associated key, and

(4) make available a decrypted version of said cryptogram.

Claim 2: The method of claim 1 wherein said decryption function makes available a plurality of said decrypted versions within each said web site page in a plurality of said web site pages in a web site,

whereby all said decrypted versions are available for display in the original position of their corresponding said cryptograms within said web site.

Claim 3: The method of claim 1 wherein said cryptogram is of any size up to the size allowed by HTML standards for the body of said web site page.

Claim 4 (previously canceled)

Claim 5: The method of claim 1 wherein said decryption function obtains said associated key from a plurality of said associated keys,

whereby each of said plurality of said web site pages contains within itself the means for independently decrypting a plurality of said cryptograms.

Claim 6: The method of claim 5 wherein a human operator provides said plurality of said associated
keys, comprising:

(a) providing a first means for sending an input request to said human operator, and

(b) providing a second means for receiving said plurality of said associated keys directly into said website page,

whereby said human operator determines which of said plurality of said cryptograms are decrypted.

Claim 7: The method of claim 6 wherein said human operator receives a validity report directly from said decryption function upon entry of each said associated key,

whereby said human operator is afforded the convenience of receiving notice of the validity of each said key from said web site page itself.

Claim 8: The method of claim 6 wherein said plurality of said associated keys are made available to said plurality of said web site pages in said web site, comprising:

(a) providing a frameset page which will establish communication between said plurality of said web site pages if not already established, and

(b) providing a third means which will distribute said plurality of said associated keys to all said web site pages as they are displayed,

whereby said human operator is afforded the convenience of entering said plurality of said associated keys in a single declaration.

Claim 9: The method of claim 6 wherein said decryption function operates only on the first instance of said cryptogram being found within said web site,

whereby said human operator is requested to enter said plurality of said associated keys only if an instance of said cryptogram is encountered while said human operator is browsing said web site.